We Claim:

1. A computer program product for use with a data forwarding computer, said computer program product comprising a computer usable medium having computer readable program code means embodied in said medium for generating an encrypted digital signature for authentication of target data by one or more of a set of recipient computers, said computer program product comprising:

computer readable program code means for causing the data forwarding computer to request a private key and an associated public key from a public key encryption system,

computer readable program code means for causing the data forwarding computer to maintain the private key in the dynamic memory of the data forwarding computer,

computer readable program code means for causing the data forwarding computer to maintain the public key in a database available to the set of recipient computers,

computer readable program code means for causing the data forwarding computer to generate a digital signature for the target data,

computer readable program code means for causing the data forwarding computer to encrypt the digital signature using the public key encryption system and the private key, and

computer readable program code means for causing the data forwarding computer to forward the target data and the encrypted digital signature to one or more of the set of recipient computers,

whereby each of the set of recipient computers is permitted to access the public key in the database to enable the decryption of the encrypted digital signature using the public key encryption system for authentication of the target data.

2. The computer program product of claim 1 further comprising computer readable program code restart means for causing the data forwarding computer to request a replacement private key and an associated replacement public key, the replacement private key being maintained in the dynamic memory of the data forwarding computer and the replacement public key being maintained in the database by the data forwarding computer, the restart means being invoked on a restart of the data forwarding computer.

3. The computer program product of claim 2, further comprising:

computer readable program code means for causing the data forwarding computer to determine an elapsed time, and

computer readable program code means for causing the data forwarding computer to purge each public key in the database that has been maintained in the database for longer than the elapsed time.

4. The computer program product of claim 3 further comprising:

computer readable program code means for causing the data forwarding computer to obtain a unique identifier, and

computer readable program code means for causing the data forwarding computer to associate the unique identifier with the target data and to forward the unique identifier with the target data.

5. The computer program product of claim 4 further comprising:

computer readable program code means for causing the data forwarding computer to maintain the unique identifier with each public key stored in the database,

whereby one of the set of recipient computers is enabled to retrieve one or more public keys from the database by specifying the unique identifier.

6. A method for generating an encrypted digital signature by a data forwarding computer, for authentication of target data by one or more of a set of recipient computers, method comprising:

the data forwarding computer:

a. requesting a private key and an associated public key from a public key encryption system,

b. maintaining the private key in the dynamic memory of the data forwarding computer,

c. maintaining the public key in a database available to the set of recipient computers,

d. generating a digital signature for the target data,

e. encrypting the digital signature using the public key encryption system and the private key, and

f. forwarding the target data and the encrypted digital signature to one or more of the set of recipient computers, and

each of the set of recipient computers receiving the target data accessing the public key in the database and decrypting the encrypted digital signature using the public key encryption system to authenticate the target data.

7. The method of claim 6 further comprising the steps of the data forwarding computer responding to a restart condition by requesting a replacement private key and an associated replacement public key, maintaining the replacement private key in the dynamic memory of the data forwarding computer and maintaining the replacement public key in the database.

8. The method of claim 7, further comprising the steps the data forwarding computer determining an elapsed time, and purging each public key in the database that has been maintained in the database for longer than the elapsed time.

9. The method of claim 7 further comprising the steps of :

the data forwarding computer obtaining a unique identifier, and

the data forwarding computer associating the unique identifier with the target data and forwarding the unique identifier with the target data.

10. The method of claim 9 further comprising the steps of the computer readable program code maintaining the unique identifier with each public key stored in the database, and one of the set of recipient computers retrieving one or more public keys from the database by specifying the unique identifier.

11. A computer program product for use with a client-server computer network, the network comprising a set of server computers and a set of client computers, said computer program product comprising a computer usable medium having computer readable program code means embodied in said medium for providing authentication of cookies, said computer program product comprising:

a. computer readable program code means for enabling a first one of the set of client computers communicating with a first one of the set of server computers to provide identifying data to the first one of the set of server computers,

b. computer readable program code means for enabling the first one of the set of server computers to request a private key and an associated public key from a public key encryption system,

c. computer readable program code means for causing the first one of the set of server computers to maintain the private key in a dynamic memory device,

d. computer readable program code means for causing the first one of the set of server computers to maintain the public key in a database available to the set of server computers,

e. computer readable program code means for enabling the first one of the set of server computers to generate a cookie for the first one of the set of client computers, the cookie comprising data corresponding to the identifying data provided by the first one of the set of client computers,

f. computer readable program code means for causing the first one of the set of server computers to generate a digital signature for the cookie,

g. computer readable program code means for causing the first one of the set of server computers to encrypt the digital signature using the public key encryption system and the private key,

h. computer readable program code means for enabling the first one of the set of server computers to forward the cookie and the associated encrypted digital signature to the first one of the set of client computers,

i. computer readable program code means for enabling the first one of the set of client computers to communicate with a second one of the set of server computers, and in response, the second one of the set of server computers to request and receive the cookie and the encrypted digital signature from the first one of the set of client computers,

j. computer readable program code means for causing the second one of the set of server computers to retrieve the public key for the encrypted digital signature from the database and to decrypt the digital signature using the public key encryption system and the retrieved public key, and

k. computer readable program code means for enabling the second one of the set of server computers to use the decrypted digital signature to authenticate the cookie received from the first one of the set of client computers.

12. The computer program product of claim 11, further comprising:

a. computer readable program code means for assigning a unique server identifier to each one of the set of server computers,

b. computer readable program code means for associating a corresponding server identifier with each public key maintained in the database, and

c. computer readable program code means for retrieving public keys in the database by reference to a server identifier.

13. The computer program product of claim 11 further comprising computer readable program code means for removing one or more public keys from the database when the one or more public keys have been maintained in the database for longer than a preselected time.

14. A method for providing authentication of cookies in a client-server computer network, the network comprising a set of server computers and a set of client computers, the method comprising the following steps:

a. a first one of the set of client computers communicating with a first one of the set of server computers, the first one of the set of client computers providing identifying data to the first one of the set of server computers,

b. the first one of the set of server computers requesting a private key and an associated public key from a public key encryption system,

c. the first one of the set of server computers maintaining the private key in a dynamic memory device,

d. the first one of the set of server computers maintaining the public key in a database available to the set of server computers,

e. the first one of the set of server computers generating a cookie for the first one of the set of client computers, the cookie comprising data corresponding to the identifying data provided by the first one of the set of client computers,

f. the first one of the set of server computers generating a digital signature for the cookie,

g. the first one of the set of server computers encrypting the digital signature using the public key encryption system and the private key,

h. the first one of the set of server computers forwarding the cookie and the associated encrypted digital signature to the first one of the set of client computers,

i. the first one of the set of client computers communicating with a second one of the set of server computers, and in response, the second one of the set of server computers requesting and receiving the cookie and the encrypted digital signature from the first one of the set of client computers,

j. the second one of the set of server computers retrieving the public key for the encrypted digital signature from the database and decrypting the digital signature using the public key encryption system and the retrieved public key,

k. the second one of the set of server computers using the decrypted digital signature to authenticate the cookie received from the first one of the set of client computers.

15. The method of claim 14 comprising the further steps of:

a. assigning a unique server identifier to each one of the set of server computers,

b. associating a corresponding server identifier with each public key maintained in the database, and

c. retrieving public keys in the database by reference to a server identifier.

16. The method of claim 14 comprising the further step of removing one or more public keys from the database when the one or more public keys have been maintained in the database for longer than a preselected time.